



p-14683-A

日 本 国 特 許 庁  
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office

出 願 年 月 日

Date of Application:

2001年 4月 2日

出 願 番 号

Application Number:

特願2001-103066

出 願 人

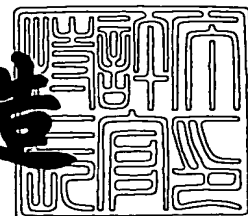
Applicant(s):

日本電信電話株式会社

2001年 6月13日

特許庁長官  
Commissioner,  
Japan Patent Office

及川耕造



出証番号 出証特2001-3055437

【書類名】 特許願

【整理番号】 NTTH127204

【提出日】 平成13年 4月 2日

【あて先】 特許庁長官殿

【国際特許分類】 G06F 15/62

【発明者】

【住所又は居所】 東京都千代田区大手町二丁目 3 番 1 号 日本電信電話株式会社内

【氏名】 斎藤 賢一

【発明者】

【住所又は居所】 東京都千代田区大手町二丁目 3 番 1 号 日本電信電話株式会社内

【氏名】 重松 智志

【発明者】

【住所又は居所】 東京都千代田区大手町二丁目 3 番 1 号 日本電信電話株式会社内

【氏名】 羽田野 孝裕

【発明者】

【住所又は居所】 東京都千代田区大手町二丁目 3 番 1 号 日本電信電話株式会社内

【氏名】 藤井 孝治

【発明者】

【住所又は居所】 東京都千代田区大手町二丁目 3 番 1 号 日本電信電話株式会社内

【氏名】 中西 衛

【発明者】

【住所又は居所】 東京都千代田区大手町二丁目 3 番 1 号 日本電信電話株式会社内

【氏名】 池田 奈美子

【特許出願人】

【識別番号】 000004226

【氏名又は名称】 日本電信電話株式会社

【代理人】

【識別番号】 100064621

【弁理士】

【氏名又は名称】 山川 政樹

【電話番号】 03-3580-0961

【手数料の表示】

【予納台帳番号】 006194

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 9701512

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 生体情報認証自動現金受け払い機

【特許請求の範囲】

【請求項 1】 利用者の生体情報の認証に基づき前記利用者に対し現金の受け払いを含むサービスを提供する生体情報認証自動現金受け払い機であって、

利用者の生体情報に基づき利用者本人の認証を行う生体情報認証トークンを備え、

前記生体情報認証トークンは、

利用者の生体情報を記憶する記憶手段と、

利用者の生体情報を検出するセンサと、

前記センサの検出情報と前記記憶手段の記憶情報との一致に基づき制御情報を出力する処理手段とを有し、

前記生体情報認証自動現金受け払い機は、

前記処理手段の制御情報に基づいて前記利用者に前記サービスを提供するサービス提供手段を有することを特徴とする生体情報認証自動現金受け払い機。

【請求項 2】 請求項 1 において、

予め利用者の口座番号に対応して残高が記憶されたデータベースを備え、

前記生体情報認証トークンの記憶手段には前記利用者の口座番号が記憶され、

前記処理手段は、前記センサの検出情報と記憶手段の記憶情報との一致に基づき前記記憶手段の口座番号を前記制御情報として出力し、

前記サービス提供手段は、

前記処理手段からの口座番号を受信すると前記データベース内の受信口座番号に対応する残高を取得する取得手段と、

前記取得手段により取得された残高から利用者の所定操作に応じた現金を引き出す引き出し手段と、

前記取得手段により取得された残高から前記引き出し手段により引き出された金額を減じて新たな残高として前記データベースに記憶する残高記録手段と

を有することを特徴とする生体情報認証自動現金受け払い機。

【請求項 3】 請求項 1 において、

予め利用者の口座番号に対応して残高が記憶されたデータベースを備え、  
前記生体情報認証トークンの記憶手段には前記利用者の口座番号が記憶され、  
前記処理手段は、前記センサの検出情報と記憶手段の記憶情報との一致に基づき前記記憶手段の口座番号を前記制御情報として出力し、  
前記サービス提供手段は、  
前記処理手段からの口座番号を受信すると前記データベース内の受信口座番号に対応する残高を取得する取得手段と、  
前記取得手段により取得された残高に対し利用者により入金された金額を加算し新たな残高として前記データベースに記憶する残高記録手段と  
を有することを特徴とする生体情報認証自動現金受け払い機。

【請求項 4】 利用者の生体情報の認証に基づき前記利用者に対し現金の受け払いを含むサービスを提供する生体情報認証自動現金受け払い機であって、  
センサにより検出された利用者の生体情報と記憶手段に記憶された生体情報との比較照合に基づき利用者本人を認証する生体情報認証トークンと情報の授受を行う情報授受手段と、

センサの検出情報と記憶手段の生体情報との一致に基づき前記生体情報認証トークンから出力される制御情報が前記情報授受手段により受信されると、この受信制御情報に基づいて前記利用者に前記サービスを提供するサービス提供手段と  
を有することを特徴とする生体情報認証自動現金受け払い機。

【請求項 5】 請求項 4 において、  
予め利用者の口座番号に対応して残高が記憶されたデータベースを備え、  
前記生体情報認証トークンの記憶手段には前記利用者の口座番号が記憶され、  
前記サービス提供手段は、  
前記センサの検出情報と記憶手段の生体情報との一致に基づき前記生体情報認証手段から前記制御情報として出力される口座番号が前記情報授受手段により受信されると、前記データベース内のこの受信口座番号に対応する残高を取得する取得手段と、  
前記取得手段により取得された残高から利用者の所定操作に応じた現金を引き出す引き出し手段と、

前記取得手段により取得された残高から前記引き出し手段により引き出された金額を減じて新たな残高として前記データベースに記憶する残高記録手段とを有することを特徴とする生体情報認証自動現金受け払い機。

【請求項 6】 請求項 4 において、

予め利用者の口座番号に対応して残高が記憶されたデータベースを備え、前記生体情報認証トークンの記憶手段には前記利用者の口座番号が記憶され、前記サービス提供手段は、

前記センサの検出情報と記憶手段の生体情報との一致に基づき前記生体情報認証手段から前記制御情報として出力される口座番号が前記情報授受手段により受信されると、前記データベース内のこの受信口座番号に対応する残高を取得する取得手段と、

前記取得手段により取得された残高に対し利用者により入金された金額を加算し新たな残高として前記データベースに記憶する残高記録手段とを有することを特徴とする生体情報認証自動現金受け払い機。

【請求項 7】 請求項 2 または 3 または 5 または 6 において、

前記残高記録手段は、利用者の預金通帳が挿入されている場合に前記残高を含む情報を前記預金通帳に記録することを特徴とする生体情報認証自動現金受け払い機。

【請求項 8】 請求項 1 ないし 7 の何れかにおいて、

前記記憶手段は利用者の指紋画像を前記生体情報として記憶し、

前記センサは利用者の指紋画像を前記生体情報として検出し、

前記処理手段または生体情報認証トークンは、前記センサにより検出された指紋画像と前記記憶手段の指紋画像との一致に基づき前記制御情報を出力することを特徴とする生体情報認証自動現金受け払い機。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明は、生体情報認証自動現金受け払い機に関する。

【0002】

## 【従来の技術】

この種の自動現金受け払い機（以下、A T M）は銀行等に設置され、利用者が自身の銀行カードをA T Mに挿入し、かつ自身のパスワード（暗証番号）を入力すると、A T Mではその利用者が銀行口座の所有者か否かを判断し、所有者と判断した場合は、利用者のお金の引き出しなど、各種サービスを提供している。

## 【0 0 0 3】

しかし、このようなA T Mでは、利用者の銀行カード及びパスワードが盗まれると、第三者により不正に利用され、セキュリティ上の問題があるため、特開昭 6 3 - 1 2 4 1 7 5 号公報に開示されているような、利用者の指紋を読み取って利用者本人か否かを認証するようにしたものがある。

## 【0 0 0 4】

このような指紋照合装置付A T Mでは、カードに記憶された登録指紋データをA T Mの指紋照合装置で読み込み、この読み込んだ指紋データと、指紋センサにより測定された指紋データとを照合することにより、その利用者が銀行口座の所有者か否かを認証し、所有者と認証した場合は、利用者のお金の引き出しなど、各種サービスを提供している。

## 【0 0 0 5】

## 【発明が解決しようとする課題】

しかしながら、前記指紋照合装置付A T Mでは、A T M内に利用者の登録指紋データが読み込まれるため、指紋データが銀行側に悪用されるのではないかという心配が利用者側に発生するという問題があった。また、指紋センサを複数の利用者が共用で用いるため、直前に利用した利用者の指紋の跡（汗などによって生じる）が指紋センサ上に残っている場合があり、このような指紋センサ上の残存指紋が利用されて容易に偽造指紋が作成されてしまうという問題もあった。

## 【0 0 0 6】

したがって、本発明は、利用者の指紋を読み取って利用者本人か否かを認証し利用者のお金の引き出しなど各種サービスを提供するA T Mにおいて、利用者の指紋データのセキュリティを向上させることを目的とする。

## 【0 0 0 7】

## 【課題を解決するための手段】

このような課題を解決するために本発明は、利用者の生体情報の認証に基づき利用者に対し現金の受け払いを含むサービスを提供する生体情報認証自動現金受け払い機であって、利用者の生体情報に基づき利用者本人を認証する生体情報認証トークンは、利用者の生体情報を記憶する記憶手段と、利用者の生体情報を検出するセンサと、センサの検出情報と記憶手段の記憶情報との一致に基づき制御情報を出力する処理手段とを有し、生体情報認証自動現金受け払い機は、処理手段の制御情報に基づき前記サービスの提供を行うサービス提供手段を有するように構成したものである。

## 【0008】

この場合、予め利用者の口座番号に対応して残高が記憶されたデータベースを備え、かつ記憶手段に利用者の口座番号を記憶するとともに、処理手段は、センサの検出情報と記憶手段の記憶情報との一致に基づき記憶手段の口座番号を制御情報として出力し、サービス提供手段は、処理手段からの口座番号を受信するとデータベース内の受信口座番号に対応する残高を取得する取得手段と、取得手段により取得された残高から利用者の所定操作に応じた現金を引き出す引き出し手段と、取得手段により取得された残高から引き出し手段により引き出された金額を減じて新たな残高としてデータベースに記憶する残高記録手段とを有するものである。

## 【0009】

また、サービス提供手段は、処理手段からの口座番号を受信するとデータベース内の受信口座番号に対応する残高を取得する取得手段と、取得手段により取得された残高に対し利用者により入金された金額を加算し新たな残高としてデータベースに記憶する残高記録手段とを有するものである。

また、残高記録手段は、利用者の預金通帳が挿入されている場合に前記残高を含む情報を預金通帳に記録するものである。

また、記憶手段に利用者の指紋画像を前記生体情報として記憶し、センサは利用者の指紋画像を前記生体情報として検出するとともに、処理手段は、センサにより検出された指紋画像と記憶手段の指紋画像との一致に基づき制御情報を出力



するように構成したものである。

#### 【 0 0 1 0 】

##### 【発明の実施の形態】

以下、本発明について図面を参照して説明する。

図 1 は、本発明に係る生体情報認証自動現金受け払い機を適用したシステムの構成を示すブロック図である。図 1 に示す自動現金受け払い機 1 0 1 は、銀行などに設置され、利用者の生体情報として利用者の指紋を照合することにより、利用者本人であるか否かを認証し、利用者本人であると認証すると利用者のお金の引き出しなど、各種サービスを提供するものである。ここで、自動現金受け払い機 1 0 1 はネットワーク 1 1 1 を介してデータベース 1 1 0 に接続される。なお、図 1 には示されていないが、データベース 1 1 0 は、サーバを介してネットワーク 1 1 1 に接続されていても良い。

#### 【 0 0 1 1 】

前記自動現金受け払い機 1 0 1 は、図 1 に示すように、後述の指紋認証トークンが差し込まれる差込口 1 0 2 が設けられ、かつ前記指紋認証トークンからの指紋情報の認証処理等を行う処理装置 1 0 3 が設けられているとともに、処理装置 1 0 3 には、記憶装置 1 0 4 と、利用者への現金の受け払いを行う現金受け払い制御装置 1 0 5 と、差込口 1 0 9 に差し込まれた通帳に残高などの記入を行う通帳記入装置 1 0 8 とが接続される構成となっている。

#### 【 0 0 1 2 】

この自動現金受け払い機 1 0 1 の前記差込口 1 0 2 に差し込まれる指紋認証トークンは、利用者が所持し、持ち運びのできる小型、軽量の装置であって、図 2 に示すように、本体部 2 0 1 が設けられているとともに、本体部 2 0 1 に、指紋センサ 2 0 2 と、処理装置 2 0 3 と、記憶装置 2 0 4 と、自動現金受け払い機 1 0 1 との接続端子である端子 2 0 5 とが設けられている。そして、処理装置 2 0 3 は、指紋センサ 2 0 2、記憶装置 2 0 4 及び端子 2 0 5 に接続されている。

#### 【 0 0 1 3 】

図 5 は前記指紋認証トークン 2 0 0 を構成する指紋センサ 2 0 2 の概略的な断面を示す図である。本指紋センサ 2 0 2 は、例えばシリコンからなる半導体基板

2 1 1 上の下層絶縁膜 2 1 2 上に形成された層間絶縁膜 2 1 4 上に、たとえば  $80\mu\text{m}$  角の複数のセンサ電極 2 1 5 と、格子状のアース電極 2 1 6 とを備え、複数のセンサ電極 2 1 5 とアース電極 2 1 6 とを、層間絶縁膜 2 1 4 表面で規定される同一平面上に配置している。

## 【 0 0 1 4 】

センサ電極 2 1 5 は、層間絶縁膜 2 1 4 上に形成されたパシベーション膜 2 1 7 で覆い、 $150\mu\text{m}$  間隔に複数個を備えるようにするとともに、Au から構成し、膜厚  $1\mu\text{m}$  程度に形成している。パシベーション膜 2 1 7 の膜厚は  $3\mu\text{m}$  程度としたので、センサ電極 2 1 5 上には、パシベーション膜 2 1 7 が約 2 ( $=3-1$ )  $\mu\text{m}$  存在している。このパシベーション膜 2 1 7 は、例えばポリイミドなどの比誘電率が 4. 0 程度の絶縁物から構成される。

## 【 0 0 1 5 】

上記下層絶縁膜 2 1 2 上には、センサ電極 2 1 5 にスルーホールを介して接続する配線 2 1 3 を形成する一方、半導体基板 2 1 1 上には、センサ電極 2 1 5 に形成される容量を検出する容量検出回路 2 1 8 を形成している。この容量検出回路 2 1 8 は、前述した配線 2 1 3 によってセンサ電極 2 1 5 に接続される。容量検出回路 2 1 8 は、センサ電極 2 1 5 毎に用意され、センサ電極 2 1 5 と認識対象（指）の一部との間に形成される容量を検出する。

## 【 0 0 1 6 】

各容量検出回路 2 1 8 の出力は、処理装置 2 0 3 に接続され、この処理装置 2 0 3 により、各センサ電極 2 1 5 に形成された容量を濃淡に変換した指紋画像データが生成される。

各容量検出回路 2 1 8、処理装置 2 0 3 及び記憶装置 2 0 4 は、たとえばセンサ電極 2 1 5 下の半導体基板 2 1 1 上に形成する。これにより指紋センサ 2 0 2、処理装置 2 0 3 及び記憶装置 2 0 4 をワンチップ化でき、したがって指紋認証トークン 2 0 0 のワンチップ化が可能になる。なお、こうしたワンチップ化の他の例として、例えば特開 2 0 0 0 - 2 4 2 7 7 1 に開示されたものがある。

## 【 0 0 1 7 】

図 6 (a) は、容量検出回路 2 1 8 の回路図である。図 6 (a) において、C

f は図 5 におけるセンサ電極 2 1 5 と指 3 の皮膚との間に形成される静電容量である。容量  $C_f$  を形成するセンサ電極 2 1 5 は NchMOS トランジスタ  $Q_{3a}$  のドレイン端子に接続されており、このトランジスタ  $Q_{3a}$  のソース端子は電流  $I$  の電流源 2 1 a の入力側に接続されている。また、センサ電極 2 1 5 とトランジスタ  $Q_{3a}$  との節点  $N_{1a}$  には、NchMOS トランジスタ（第 1 の素子） $Q_{2a}$  のソース端子が接続されている。このトランジスタ  $Q_{2a}$  のドレイン端子には、ソース端子に電源電圧  $V_{DD}$  が印加された PchMOS トランジスタ（第 1 のスイッチ手段） $Q_{1a}$  のドレイン端子と、ドレイン端子に電源電圧  $V_{DD}$  が印加されソース端子が抵抗  $R_a$  を介して接地に接続された NchMOS トランジスタ  $Q_{4a}$  のゲート端子とが接続されている。このトランジスタ  $Q_{4a}$  のソース端子にインバータゲート 4 1 が接続されている。

## 【 0 0 1 8 】

各トランジスタ  $Q_{1a}$ 、 $Q_{3a}$  のゲート端子にはそれぞれ信号  $PRE$ （バー）、 $RE$  が印加される。また、トランジスタ  $Q_{2a}$  のゲート端子には定電圧源からバイアス電圧  $V_G$  が印加される。ここで、トランジスタ  $Q_{2a}$  が非導通状態になるゲート－ソース間のしきい値電圧を  $V_{th}$  とすると、 $V_{DD} > V_G - V_{th}$  となるように電圧  $V_{DD}$ 、 $V_G$  が設定される。

また、節点  $N_{1a}$ 、 $N_{2a}$  はそれぞれ寄生容量  $C_{p1a}$ 、 $C_{p2a}$  を有している。

## 【 0 0 1 9 】

図 6（b）～図 6（d）は、図 6（a）に示した容量検出回路 2 1 8 の動作を説明するためのタイミングチャートであり、図 6（b）はトランジスタ  $Q_{1a}$  を制御する信号  $PRE$ （バー）の電位変化を示し、図 6（c）はトランジスタ  $Q_{3a}$  を制御する信号  $RE$  の電位変化を示し、図 6（d）は節点  $N_{1a}$ 、 $N_{2a}$  それぞれの電位変化を示している。

最初、トランジスタ  $Q_{1a}$  のゲート端子には  $High$  レベル（ $V_{DD}$ ）の信号  $PRE$ （バー）が与えられ、トランジスタ  $Q_{3a}$  のゲート端子には  $Low$  レベル（ $GND$ ）の信号  $RE$  が与えられている。したがって、このときトランジスタ  $Q_{1a}$ 、 $Q_{3a}$  はともに導通していない。

## 【0020】

この状態で信号PRE（バー）がHighレベルからLowレベルに変化すると、トランジスタQ1aが導通状態になる。このときトランジスタQ3aは非導通状態のままであり、信号発生回路20は停止状態にあるから、節点N2aの電位がVDDにプリチャージされる。

また、トランジスタQ2aのゲートソース間電圧がしきい値電圧 $V_{th}$ に達してトランジスタQ2aが非導通状態になるまで、節点N1aが充電される。これにより、節点N1aの電位が $V_G - V_{th}$ にプリチャージされる。

## 【0021】

プリチャージが終了した後、信号PRE（バー）がHighレベルに変化すると、トランジスタQ1aが非導通状態になる。これと同時に信号REがHighレベルに変化すると、トランジスタQ3aが導通状態になり、信号発生回路20が動作状態に変化する。そして、電流源21aにより節点N1aに充電された電荷が引き抜かれ、節点N1aの電位がわずかに低下すると、トランジスタQ2aのゲートソース間電圧がしきい値電圧 $V_{th}$ より大きくなり、トランジスタQ2aが導通状態に変化する。これにより節点N2aの電荷も引き抜かれ、節点N2aの電位低下が開始する。

信号REをHighレベルにする期間を $\Delta t$ とすると $\Delta t$ 経過後の節点N1aの電位低下 $\Delta V$ は $V_{DD} - (V_G - V_{th}) + I \Delta t / (C_f + C_{p1a})$ になる。ここで、寄生容量 $C_{p2a}$ は寄生容量 $C_{p1a}$ に対して十分小さいとしている。

## 【0022】

電流源21aの電流 $I$ と期間 $\Delta t$ と寄生容量 $C_{p1a}$ 、 $C_{p2a}$ は、各々一定であるから、電位低下 $\Delta V$ は、センサ電極215と検出対象である指の表面3との間に発生する容量の値 $C_f$ によって決定される。この容量値 $C_f$ はセンサ電極215と指の表面3との距離によって決まるので、指紋の凹凸によって異なる。このことから、低下電位 $\Delta V$ の大きさが、指紋の凹凸を反映して変化する。この電位低下 $\Delta V$ が、入力信号として出力回路40に供給されるので、出力回路40で $\Delta V$ が入力され、指紋の凹凸を反映した信号が出力回路40から出力される。

こうした各容量検出回路218の出力信号が処理装置203により処理され、

前述の指紋画像データとして生成される。

#### 【 0 0 2 3 】

次に、以上のように構成された指紋センサ 2 0 2 を有する指紋認証トークン 2 0 0、及び指紋認証トークン 2 0 0 の指紋情報の認証に基づき現金の受け払いを行う自動現金受け払い機 1 0 1 の動作を図 3、図 4 のフローチャートに基づいて説明する。

#### （第 1 の実施の形態）

まず、図 3 のフローチャートに示す第 1 の実施の形態の動作から説明する。第 1 の実施の形態は、利用者の現金引き出しに対応する動作を示すものである。

利用者が自動現金受け払い機 1 0 1 から現金の引き出しを行う場合は、ステップ S 1 で自身の預金通帳を差込口 1 0 9 に差し込む。ここで、利用者が自身の通帳に残高などの記帳が不要な場合はステップ S 1 の動作は省略される。続いて利用者は自身の所持する指紋認証トークン 2 0 0 を差込口 1 0 2 に差込み（ステップ S 2）、さらにその指紋認証トークン 2 0 0 の指紋センサ 2 0 2 上に自身の指をのせる（ステップ S 3）。

#### 【 0 0 2 4 】

すると、指紋認証トークン 2 0 0 の処理装置 2 0 3 は、指紋センサ 2 0 2 により検出された指紋画像を読み取って画像データとして処理し、その指紋画像データの中から特徴となるデータを照合情報として抽出する（ステップ S 4）。ここで、指紋認証トークン 2 0 0 の記憶装置 2 0 4 には、予め指紋センサ 2 0 2 により検出され処理装置 2 0 3 により処理された利用者自身の指紋画像データ中の特徴部分を示す照合情報が登録されており、処理装置 2 0 3 は、記憶装置 2 0 4 に保存されているこの登録情報とステップ S 4 で抽出した照合情報とを比較する（ステップ S 5）。

#### 【 0 0 2 5 】

そして、双方の照合情報が不一致の場合はそのまま処理を終了するが、双方の照合情報が一致してステップ S 6 の「照合情報が一致？」の判定が Y E S となると、処理装置 2 0 3 は、予め記憶装置 2 0 4 内に保存されているその利用者の銀行口座番号を自動現金受け払い機 1 0 1 の処理装置 1 0 3 に送信する（ステップ

S7)。ここで、データベース110内には各利用者の口座番号に対応して残高が記憶されており、自動現金受け払い機101の処理装置103は指紋認証トークン200から口座番号が送信されてくると、この口座番号を受信し受信した口座番号に対応する残高をネットワーク111を介してデータベース110から取得し、記憶装置104に記憶する（ステップS8）。

#### 【0026】

そして、利用者がキーボード107を操作して自身の引き出し金額を入力すると（ステップS9）、自動現金受け払い機101の処理装置103は、記憶装置104に記憶された残高と、利用者の入力操作に基づく引き出し金額との大小を比較する（ステップS10）。ここで、残高が引き出し金額未満でステップS11の「残高が引き出し金額以上か？」の判定がNOとなる場合は、そのまま処理を終了するが、残高が引き出し金額以上でありステップS11の判定がYESとなると、現金受け払い制御装置105を制御することにより、引き出し金額に相当する現金を現金受け払い口106へ排出させる（ステップS12）。

#### 【0027】

この場合、自動現金受け払い機101の処理装置103は、記憶装置104に記憶された残高から引き出し金額を差し引いた残高をネットワーク111を介してデータベース110に書き込む（ステップS13）。その後、利用者による指紋認証トークン200の差込口102からの引き抜きが行われ（ステップS14）、利用者の預金通帳が差し込まれている場合は、処理装置103は通帳記入装置108を制御して利用者の現金引き出し額などを預金通帳に記録させる（ステップS15）。

#### 【0028】

このように、第1の実施の形態では、利用者がそれぞれ所有する指紋トークン200に利用者自身の指紋データを登録するとともに、利用者の口座番号を記憶し、指紋トークン200の指紋センサ202が読み取った指紋データと、登録データとが一致すると、記憶している口座番号を自動現金受け払い機101へ送信し、自動現金受け払い機101では、この口座番号を受信するとデータベース110からこの口座番号に対応する残高を取得し、この残高に応じた現金の払い出

しを行うようにしたものである。この結果、従来の自動現金受け払い機のように、利用者の登録指紋データが内部に読み込まれないため、指紋データが銀行側に悪用されるといった心配を利用者に抱かせるという問題を回避できる。また、従来の自動現金受け払い機のように、指紋センサを複数の利用者が共用で使用されることがないことから、指紋センサ上の残存指紋が第三者により不正に利用されて容易に偽造指紋が作成されてしまうという問題も回避できる。

## 【 0 0 2 9 】

なお、本実施の形態では、指紋認証トークン 2 0 0 の記憶装置 2 0 4 に、利用者の指紋データ及び口座番号を登録するように構成したが、記憶装置 2 0 4 には、この他に、利用者の氏名、住所、電話番号、預金情報等の利用者個人の情報を記憶するようにしてもよい。これにより、振込サービスの利用時には、振込元の氏名、住所、電話番号が自動的に付加されるなど、種々のサービスに個人情報を利用することができる。

## 【 0 0 3 0 】

## (第 2 の実施の形態)

次に、図 4 は第 2 の実施の形態を示すフローチャートであり、第 2 の実施の形態は、利用者の現金預け入れに対応する動作を示すものである。

利用者が自動現金受け払い機 1 0 1 に自身の現金を預け入れする場合は、ステップ S 2 1 で自身の預金通帳を差込口 1 0 9 に差し込む。ここで、利用者が自身の預金通帳に記帳が不要な場合はステップ S 2 1 の動作は省略される。続いて利用者は自身の所持する指紋認証トークン 2 0 0 を差込口 1 0 2 に差し込む（ステップ S 2 2）。

## 【 0 0 3 1 】

すると、指紋認証トークン 2 0 0 の処理装置 2 0 3 は、予め記憶装置 2 0 4 内に保存されているその利用者の銀行口座番号を自動現金受け払い機 1 0 1 の処理装置 1 0 3 に送信する（ステップ S 2 3）。処理装置 1 0 3 は口座番号を受信すると、データベース 1 1 0 からこの口座番号に対応する残高を取得し記憶装置 1 0 4 に記憶する（ステップ S 2 4）とともに、現金受け払い口 1 0 6 を開口する。この現金受け払い口 1 0 6 の開口により、利用者は自身の現金を現金受け払い

口106から入金する（ステップS25）。

【0032】

この場合、自動現金受け払い機101の処理装置103は、記憶装置104に保存されている利用者の残高にステップS24で入金された金額を加算して、その合計金額を新たな残高として、データベース110の前記口座番号に対応して記録する（ステップS26）。その後、利用者による指紋認証トークン200の差込口102からの引き抜きが行われ（ステップS27）、利用者の預金通帳が差し込まれている場合は、処理装置103は通帳記入装置108を制御して利用者の現金入金額などを預金通帳に記録させる（ステップS28）。

【0033】

なお、第2の実施の形態では、自動現金受け払い機101に指紋認証トークン200が差し込まれると、指紋認証トークン200は利用者の口座番号を自動現金受け払い機101側へ送信しているが、この場合、指紋センサ202で利用者の指紋画像を読み取り、読み取った指紋データと記憶装置204の登録指紋データとの一致に基づき利用者の口座番号を自動現金受け払い機101側へ送信するようにしても良い。このように構成することにより現金預入時のセキュリティが向上する。

【0034】

以上、図3及び図4のフローチャートを参照して本発明の要部動作を説明したが、各ステップの実行順序を入れ替えても全体の動作に矛盾を生じない場合は各ステップの順序を適宜入れ替えてもよい。

また、本実施の形態では、自動現金受け払い機101による現金の引き出し及び現金の預け入れの各動作を説明したが、振り込みや振り替えなどの他のサービスに適用しても同等の効果を奏する。

また、本実施の形態では、指紋認証トークン200を用いて本人認証を行うことにより、自動現金受け払い機の利用許可を与えているため、銀行カード及びパスワードが不要になり、セキュリティが向上する。

【0035】

また、本実施の形態では、指紋認証トークン200内の指紋センサ201，処



理装置 2 0 3, 記憶装置 2 0 4 をワンチップで構成した第 1 の構成例について説明したが、上記第 1 の構成例の他に、指紋センサ 2 0 2 をワンチップ化し、このワンチップ指紋センサ 2 0 2 に、バスを介して処理装置 2 0 3 を接続し、さらに処理装置 2 0 3 にバスを介して記憶装置 2 0 4 を接続する第 2 の構成例がある。さらに、指紋センサ 2 0 2 と処理装置 2 0 3 をワンチップ化し、このワンチップ化された処理装置 2 0 3 にバスを介して記憶装置 2 0 4 を接続する第 3 の構成例がある。

## 【 0 0 3 6 】

また、指紋認証トークン 2 0 0 と自動現金受け払い機 1 0 1 間で送受される信号を送信側で暗号化し、受信側でその暗号化データを復号化することにより、システムのセキュリティを向上させることができる。

また、本実施の形態では、指紋の認証に基づいて現金の引き出しを行うようにしたが、指の大きさ、手形、静脈パターン、人相、虹彩及び声紋などの利用者固有の生体情報や、利用者のサイン（筆跡）等により利用者本人であることを認証して現金引き出しを許容するようにしても良い。

## 【 0 0 3 7 】

図 7 は、前述の指紋認証トークン 2 0 0 を含む認証トークン 3 0 0 と、認証トークン 3 0 0 の認証を利用してユーザ（利用者）にサービスを提供する前述の自動現金受け払い機 1 0 1 を含む利用機器 4 0 0 とからなる一般的な認証システムの構成を示すブロック図である。

この認証システムでは、ユーザ固有の生体情報として指紋を用いる場合を例として説明する。

## 【 0 0 3 8 】

認証トークン 3 0 0 には、指紋（生体情報）を読み取るセンサ 3 1 1（図 2 の指紋センサ 2 0 2 に対応）、ユーザ本人の登録指紋データ 3 1 2 A やユーザ情報 3 1 2 B を記憶する記憶回路 3 1 2（図 2 の記憶装置 2 0 4 に対応）、センサ 3 1 1 での読み取り結果を示すセンシングデータ 3 1 1 A を、記憶回路 3 1 2 に記憶されている登録指紋データ 3 1 2 A を用いて照合する照合回路 3 1 3（図 2 の処理装置 2 0 3 に対応）、この照合回路 3 1 3 での照合結果を含む認証データ 3

1 3 A を通信データ 3 0 1 A として認証トークン 3 0 0 の外部へ送信する通信回路 3 1 4 (図 2 の処理装置 2 0 3 に対応) が設けられており、これら回路部を一体として形成する認証トークン 3 0 0 が利用機器 4 0 0 に対して着脱自在に接続される。

利用機器 4 0 0 には、認証トークン 3 0 0 からの通信データ 3 0 1 A を受信する通信回路 4 2 1 と、受信した通信データ 3 0 1 A に含まれる照合結果が一致を示す場合にのみ、そのユーザへのサービス提供を行う処理装置 4 2 2 とが設けられている。

#### 【 0 0 3 9 】

次に、図 7 に示す認証システムの動作について説明する。

ユーザは事前に、自分の所持する認証トークン 3 0 0 の記憶回路 3 1 2 に、自分の登録指紋データ 3 1 2 A やサービスを利用するためのパスワードや個人情報などからなるユーザ情報 3 1 2 B を記憶させておく。

利用機器 4 0 0 を利用する際、まずユーザは自分の認証トークン 3 0 0 を利用機器 4 0 0 へ接続し、指をそのセンサ 3 1 1 へ置く。これにより認証トークン 3 0 0 のセンサ 3 1 1 でユーザの指紋が読み取られセンシングデータ 3 1 1 A として出力される。このセンシングデータ 3 1 1 A は照合回路 3 1 3 において記憶回路 3 1 2 の登録指紋データ 3 1 2 A を用いて照合される。そして、その照合結果を含む認証データ 3 1 3 A が出力される。このとき照合回路 3 1 3 は、予め記憶回路 3 1 2 に格納されているユーザ ID、パスワード、個人情報などのユーザ情報 3 1 2 B を読み出し、認証データ 3 1 3 A へ含めて出力する。

#### 【 0 0 4 0 】

通信回路 3 1 4 では、照合回路 3 1 3 からの認証データ 3 1 3 A を通信データ 3 0 1 A として利用機器 4 0 0 へ送信する。

利用機器 4 0 0 の通信回路 4 2 1 では、認証トークン 3 0 0 の通信回路 3 1 4 から送信された通信データ 3 0 1 A を受信し、認証データ 3 1 3 A と同じ内容の認証データ 4 2 1 A として出力する。処理装置 4 2 2 では、この認証データ 4 2 1 A を受け取ってその認証データ 4 2 1 A に含まれる照合結果を参照する。そして、その照合結果が一致を示す場合、処理装置 4 2 2 においてユーザの所望する

所定の処理が実行される。

【 0 0 4 1 】

このように、ユーザの指紋を検出しその検出結果をセンシングデータとして出力するセンサ 3 1 1 と、ユーザの指紋を照合するための登録指紋データ 3 1 2 A が予め格納されている記憶回路 3 1 2 と、この記憶回路 3 1 2 に記憶されている登録指紋データ 3 1 2 A を用いてセンサ 3 1 1 からのセンシングデータ 3 1 1 A を照合し、ユーザ認証結果となるその照合結果を認証データとして出力する照合回路 3 1 3 と、この照合回路 3 1 3 からの認証データを通信データ 3 0 1 A として利用機器 4 0 0 へ送信する通信回路 3 1 4 とを、認証トークン 3 0 0 として一体として形成したものである。

【 0 0 4 2 】

そして、認証に応じて所定の処理を行う利用機器 4 0 0 をユーザが利用する場合には、認証トークン 3 0 0 をその利用機器 4 0 0 へ接続し、その認証トークン 3 0 0 でユーザの生体情報に基づきユーザ認証を行い、利用機器 4 0 0 へ通知するようにしたものである。

また、利用機器 4 0 0 に、認証トークン 3 0 0 から送信された通信データ 3 0 1 A を受信し認証データ 4 2 1 A として出力する通信回路 4 2 1 と、この通信回路 4 2 1 からの認証データ 4 2 1 A に含まれる照合結果に基づき所定の処理を行う処理装置 4 2 2 とを設け、この利用機器 4 0 0 とは独立した各ユーザが個々の持つ認証トークン 3 0 0 での認証結果に基づき所定の処理を行うようにしたものである。

【 0 0 4 3 】

したがって、ユーザの生体情報を検出するセンサや照合を行う照合回路を利用機器内部に設け、ユーザの登録データをデータカードでユーザ自身が所持し管理する場合と比較して、登録データが認証トークンの外部へ出力されることがなくなり照合時に用いる登録データの漏洩を防止できる。また、センサを不特定多数のユーザで共用する必要がなく、ユーザが個々に所持する認証トークンごとに設けられているセンサを用いるため、センサ故障が発生しても他のユーザには波及せず、さらに生体情報検出の際、指紋などのようにセンサに対して人体の一部を

接触させる必要がある場合でもユーザに対して良好な衛生環境を保つことができる。なお、認証トークン 3 0 0 については、センサ、記憶回路および照合回路などを 1 チップの半導体装置として形成する技術（例えば、特開 2 0 0 0 - 2 4 2 7 7 1 号公報など参照）を用いることで、非常に小型な認証トークンを実現することも可能となる。

## 【 0 0 4 4 】

さらに、記憶回路 3 1 2 にユーザ ID やパスワードさらには個人情報などのユーザ情報 3 1 2 B を予め記憶しておき、これらを認証データ 3 1 3 A に含めて利用機器 4 0 0 へ送信するようにしたので、利用機器 4 0 0 の処理装置 4 2 2 において、その認証データに含まれるユーザ情報 3 1 2 B、例えばユーザ ID やパスワードをチェックすることにより処理実行の可否を判断でき、利用機器で行う処理の重要性に合わせた基準で認証判定できる。また、ユーザ情報 3 1 2 B の個人情報、例えば氏名、住所、電話番号、口座番号やクレジットカード番号などを処理に用いることにより、処理に必要な個人情報をユーザが入力する必要がなくなり、ユーザの操作負担を大幅に軽減できる。

## 【 0 0 4 5 】

なお、利用機器 4 0 0 に図示しない乱数発生回路及び復号回路を設け、かつ認証トークン 3 0 0 に図示しない暗号化回路を設けて、利用機器 4 0 0 と認証トークン 3 0 0 間で通信されるデータの暗号化することにより、セキュリティの向上を図ることができる。

## 【 0 0 4 6 】

即ち、利用機器 4 0 0 は、認証トークン 3 0 0 側からのアクセス時に乱数発生回路により乱数を発生させてこの乱数を通信回路 4 2 1 から認証トークン 3 0 0 へ送信して暗号化回路に記憶させる一方、認証トークン 3 0 0 の暗号化回路は照合回路 3 1 3 から出力された認証データ 3 1 3 A と、記憶した乱数との和を演算してその演算結果を、予め記憶回路 3 1 2 に記憶してある共通鍵により暗号化して暗号化データとして利用機器 4 0 0 側へ送信する。利用機器 4 0 0 では、通信回路 4 2 1 により受信したこの暗号化データを復号回路が共通鍵を用いて復号化するとともに復号化したデータから乱数発生回路が発生した前記乱数を減算する

ことにより認証データ 4 2 1 A として処理回路 4 2 2 へ出力する。なお、上記の例では、認証トークン 3 0 0 及び利用機器 4 0 0 の双方に共通鍵を持たせて、それぞれ暗号化及び復号化を行わせているが、認証トークン 3 0 0 に秘密鍵を、利用機器 4 0 0 に公開鍵を持たせてそれぞれ暗号化処理及び復号化処理を行わせることもできる。

#### 【 0 0 4 7 】

次に、図 8 を参照して、本認証システムの第 2 の構成例について説明する。図 8 は、図 7 に示す第 1 の構成例のうち、認証トークン 3 0 0 の出力段にデータ変換モジュール 3 3 0 を付加したものである。

このデータ変換モジュール 3 3 0 には、認証トークン 3 0 0 の通信回路 3 1 4 から出力された通信データを、利用機器 4 0 0 で受信・解読可能なデータ形式へ変換するプロトコル変換回路 3 3 1 が設けられている。

#### 【 0 0 4 8 】

このように、認証トークン 3 0 0 に着脱自在に取り付けられるデータ変換モジュール 3 3 0 を介して、所望の利用機器 4 0 0 と認証トークン 3 0 0 とを接続するようにしたので、データ形式が異なる利用機器に対しても同一認証トークンを用いたユーザ認証が可能となる。また、様々な形式に対応したデータ変換モジュールを用意し、それらを認証トークンに対して容易に着脱交換することで、ユーザが 1 つの認証トークンを用いて様々な利用機器を利用することができ、複数の認証トークンを所持する必要がない。

以上では、データ変換モジュール 3 3 0 を認証トークン 3 0 0 に対して着脱自在に取り付ける場合を例として説明したが、認証トークン 3 0 0 内部にプロトコル変換回路 3 3 1 を設けてもよく、さらにコンパクトに構成できる。

#### 【 0 0 4 9 】

次に、図 9 を参照して、本認証システムの第 3 の構成例について説明する。図 9 は、図 7 に示す第 1 の構成例のうち、認証トークン 3 0 0 の出力段に無線モジュール 3 4 0 を付加したものである。

この無線モジュール 3 4 0 には、認証トークン 3 0 0 の通信回路 3 1 4 から出力された通信データを、利用機器 4 0 0 で受信・解読可能なデータ形式へ変換す

るプロトコル変換装置 3 4 1 と、このプロトコル変換装置 3 4 1 からの通信データを無線区間を介して利用機器 4 0 0 へ送信する無線回路 3 4 2 とが設けられている。この場合、利用機器 4 0 0 側にも無線回路 4 2 3 を設ける必要がある。

#### 【 0 0 5 0 】

このように、認証トークン 3 0 0 に着脱自在に取り付けられる無線モジュール 3 4 0 を用いて、所望の利用機器 4 0 0 と認証トークン 3 0 0 とを接続するようにしたので、ユーザは、認証トークン 3 0 0 を利用機器 4 0 0 に直接接続することなく、例えば自分の手元で認証トークン 3 0 0 を用いてユーザ認証を行いサービスを受けることが可能となる。したがって、利用機器 4 0 0 に対して認証トークン 3 0 0 を接続する作業や、利用機器 4 0 0 に接続されている状態の認証トークン 3 0 0 を用いて認証を行う作業など、認証時のユーザに対する作業負担を大幅に軽減できる。

#### 【 0 0 5 1 】

なお、利用機器 4 0 0 と認証トークン 3 0 0 の通信プロトコルが同一の場合は、無線モジュール 3 4 0 のプロトコル変換回路 3 4 1 を省略することも可能である。また、無線回路 3 4 2 の代わりに、赤外線通信回路や超音波通信回路など、無線区間を介してデータ通信可能な通信回路を用いてもよい。

以上では、無線モジュール 3 4 0 を認証トークン 3 0 0 に対して着脱自在に取り付ける場合を例として説明したが、認証トークン 3 0 0 内部に無線回路 3 4 2 やプロトコル変換回路 3 4 1 を設けてもよく、さらにコンパクトに構成できる。

#### 【 0 0 5 2 】

##### 【発明の効果】

以上説明したように本発明は、利用者の指紋画像等の生体情報の認証に基づき利用者に対しサービスを提供する生体情報認証自動現金受け払い機であって、利用者の生体情報に基づき利用者本人を認証する生体情報認証トークンを備え、前記生体情報認証トークンは利用者の生体情報を記憶する記憶手段と、利用者の生体情報を検出するセンサと、センサの検出情報と記憶手段の記憶情報との一致に基づき制御情報を出力する処理手段とを有し、処理手段の制御情報に基づき利用者に現金の受け払いを含む前記サービスを提供するようにしたので、従来の自動

現金受け払い機のように、利用者の登録指紋データが内部に読み込まれないため、指紋データが銀行側に悪用されるといった心配を利用者に抱かせるという問題を回避できる。また、従来の自動現金受け払い機のように、指紋センサを複数の利用者が共用で使うことがないことから、指紋センサ上の残存指紋が第三者により不正に利用されて容易に偽造指紋が作成されてしまうという問題も回避できる。

【図面の簡単な説明】

【図 1】 本発明に係る自動現金受け払い機を適用したシステムの構成を示すブロック図である。

【図 2】 前記自動現金受け払い機に用いられる指紋認証トークンの外観を示す図（図 2（a））及びその構成を示すブロック図（図 2（b））である。

【図 3】 現金引き出しの際の前記自動現金受け払い機及び指紋認証トークンの動作を示すフローチャートである。

【図 4】 現金預け入れの際の前記自動現金受け払い機の動作を示すフローチャートである。

【図 5】 前記指紋認証トークンを構成する指紋センサの詳細構成を示す図である。

【図 6】 前記指紋センサ内の容量検出回路の回路図及び前記容量検出回路の各部の動作タイミングを示すタイムチャートである。

【図 7】 認証トークンおよび利用機器からなる認証システムの第 1 の構成例を示すブロック図である。

【図 8】 認証トークンおよび利用機器からなる認証システムの第 2 の構成例を示すブロック図である。

【図 9】 認証トークンおよび利用機器からなる認証システムの第 3 の構成例を示すブロック図である。

【符号の説明】

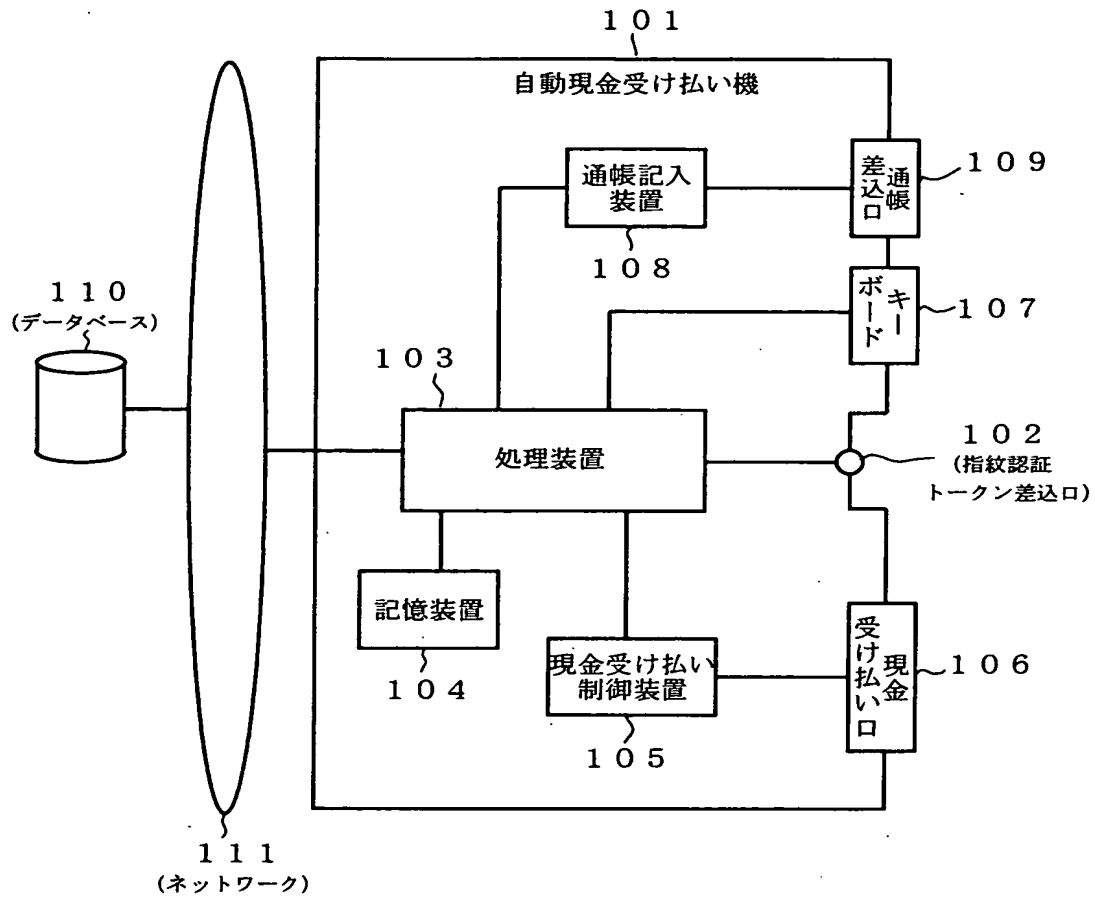
1 0 1 … 自動現金受け払い機、1 0 2 … 指紋認証トークン差込口、1 0 3, 2 0 3 … 処理装置、1 0 4, 2 0 4 … 記憶装置、1 0 5 … 現金受け払い制御装置、1 0 6 … 現金受け払い口、1 0 7 … キーボード、1 0 8 … 通帳記入装置、1 1 0

…データベース、200…指紋認証トークン、202…指紋センサ、203…処理装置、204…記憶装置、211…半導体基板、212…下層絶縁膜、213…配線、214…層間絶縁膜、215…センサ電極、217…パシベーション膜、218…容量検出回路。

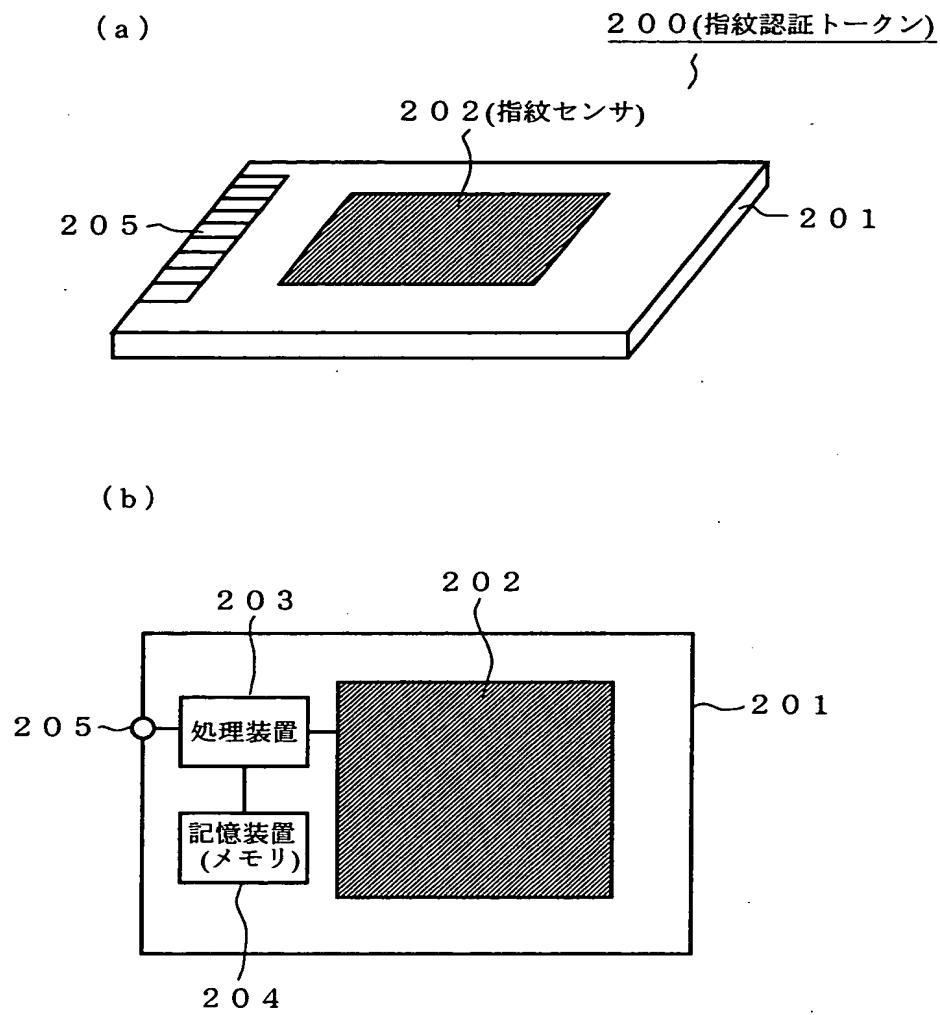


【書類名】 図面

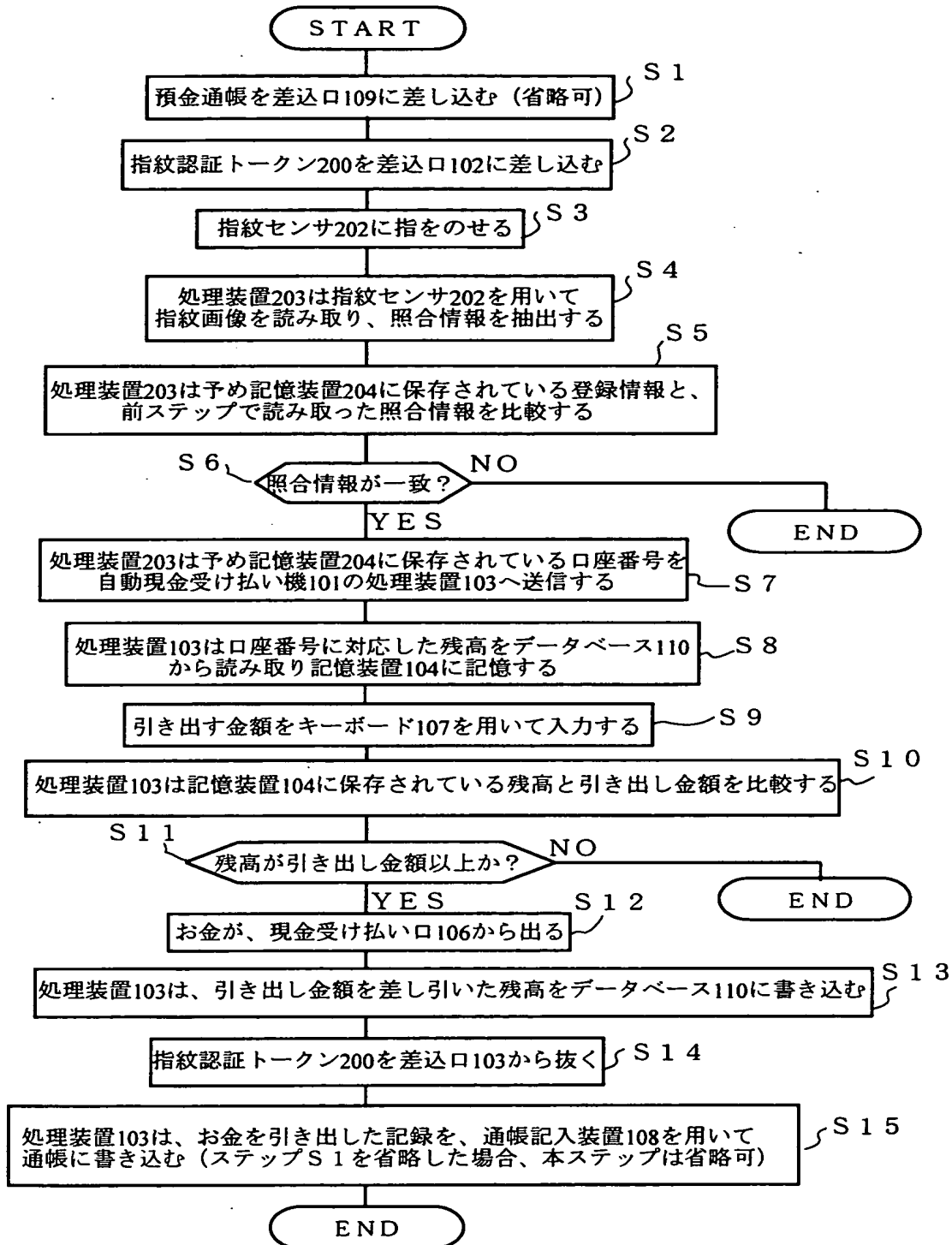
【図 1】



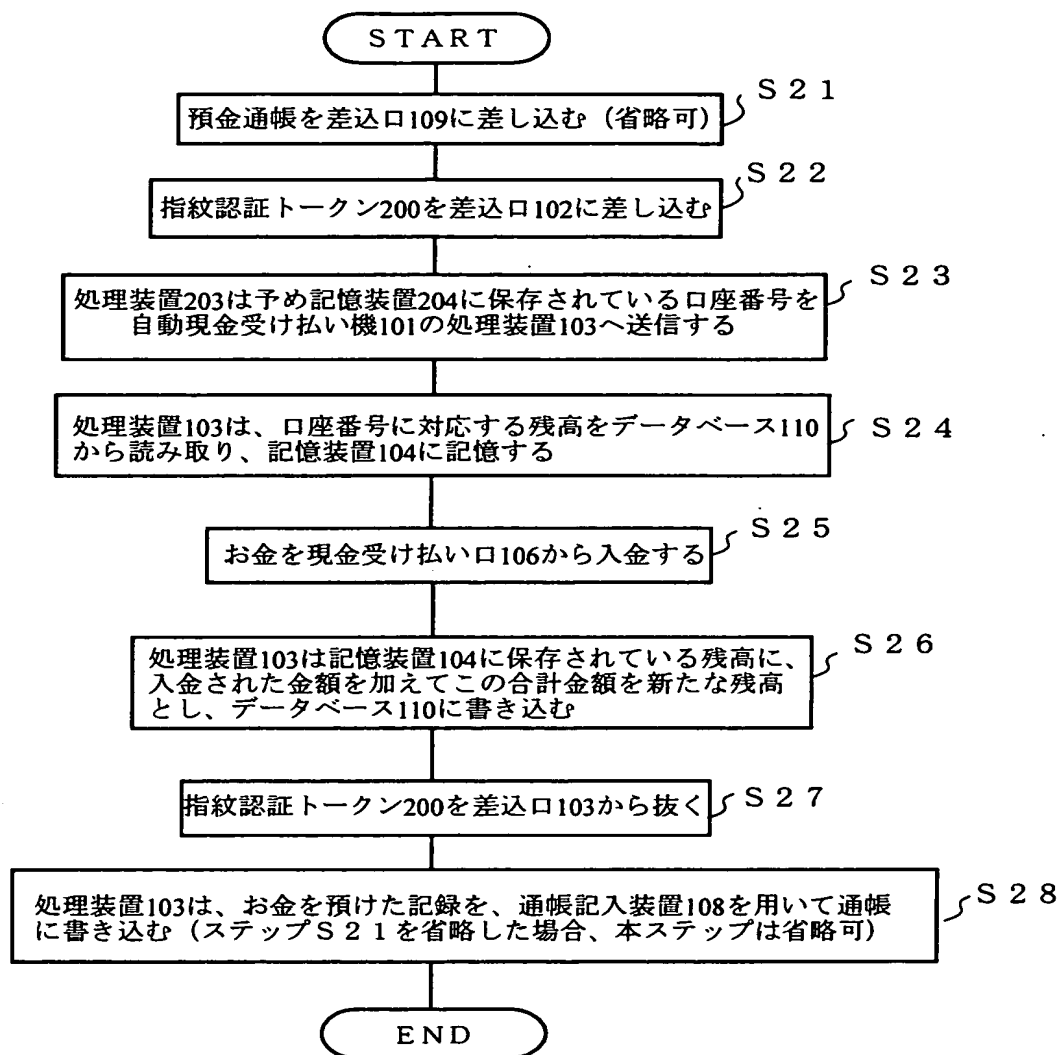
【図 2】



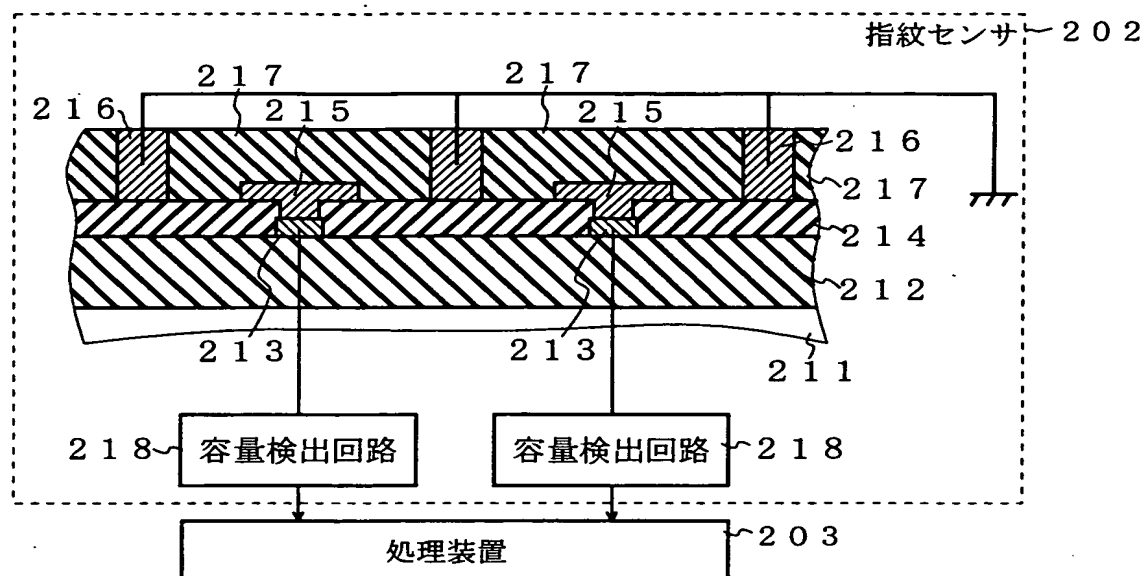
【図 3】



【図 4】

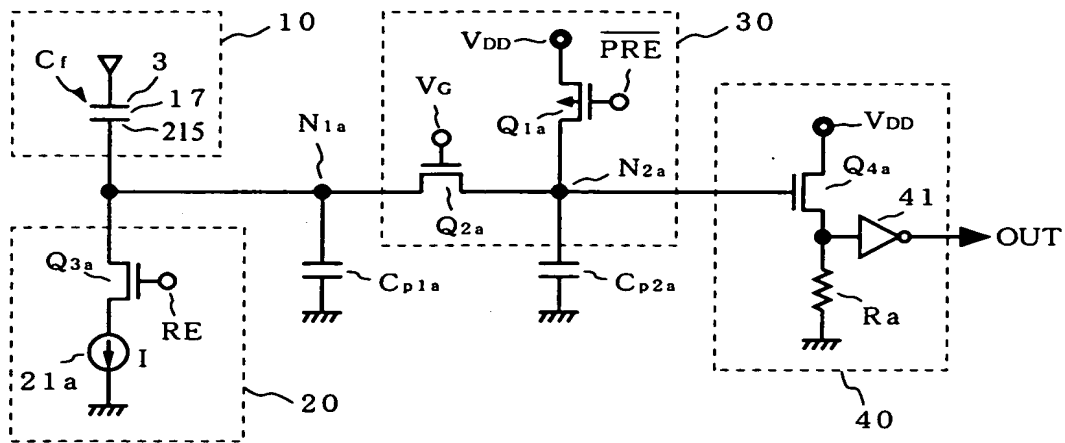


【図 5】

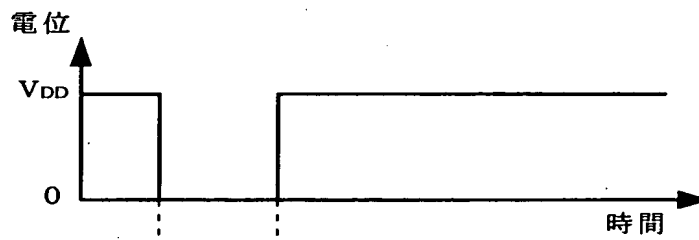


【図 6】

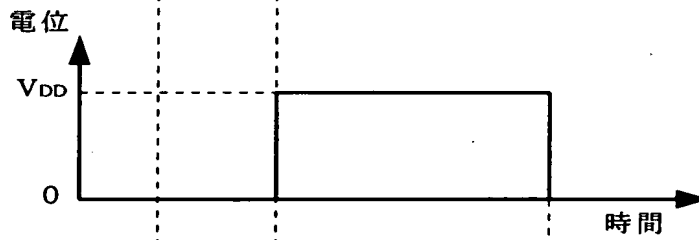
(a)



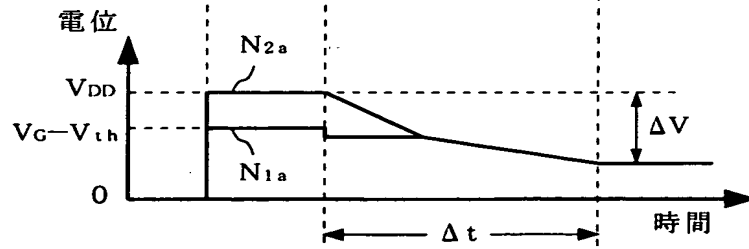
(b)  $\overline{PRE}$



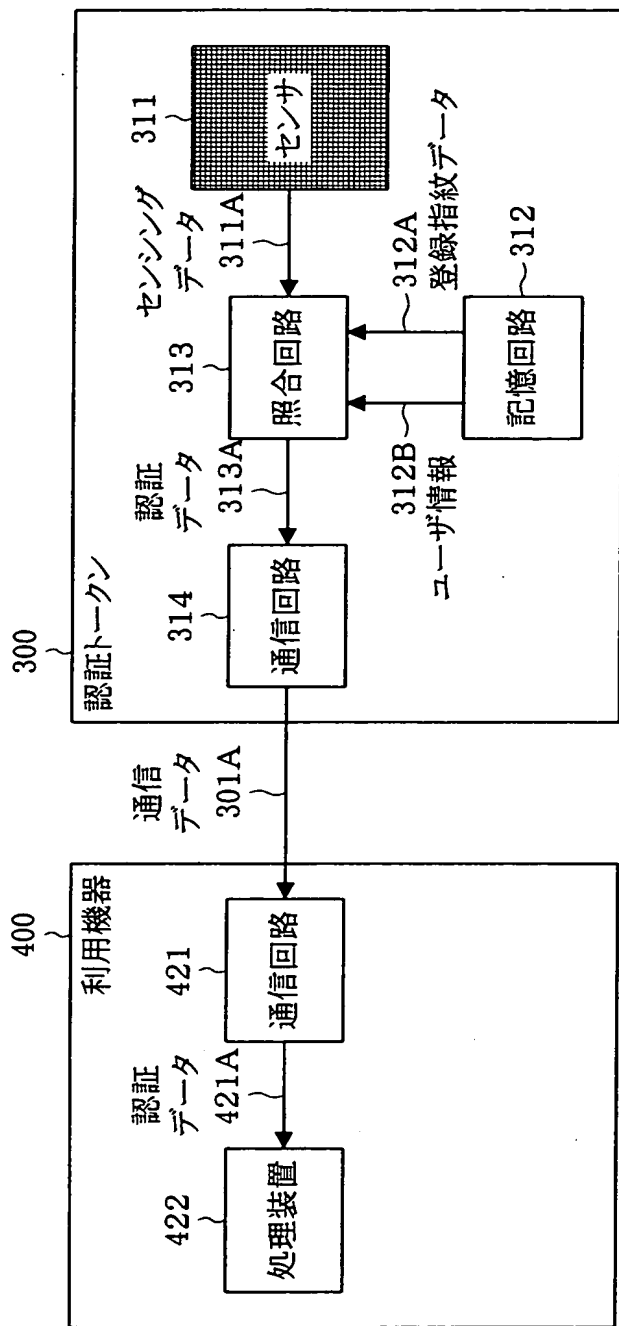
(c)  $RE$



(d)  $N_{1a}, N_{2a}$



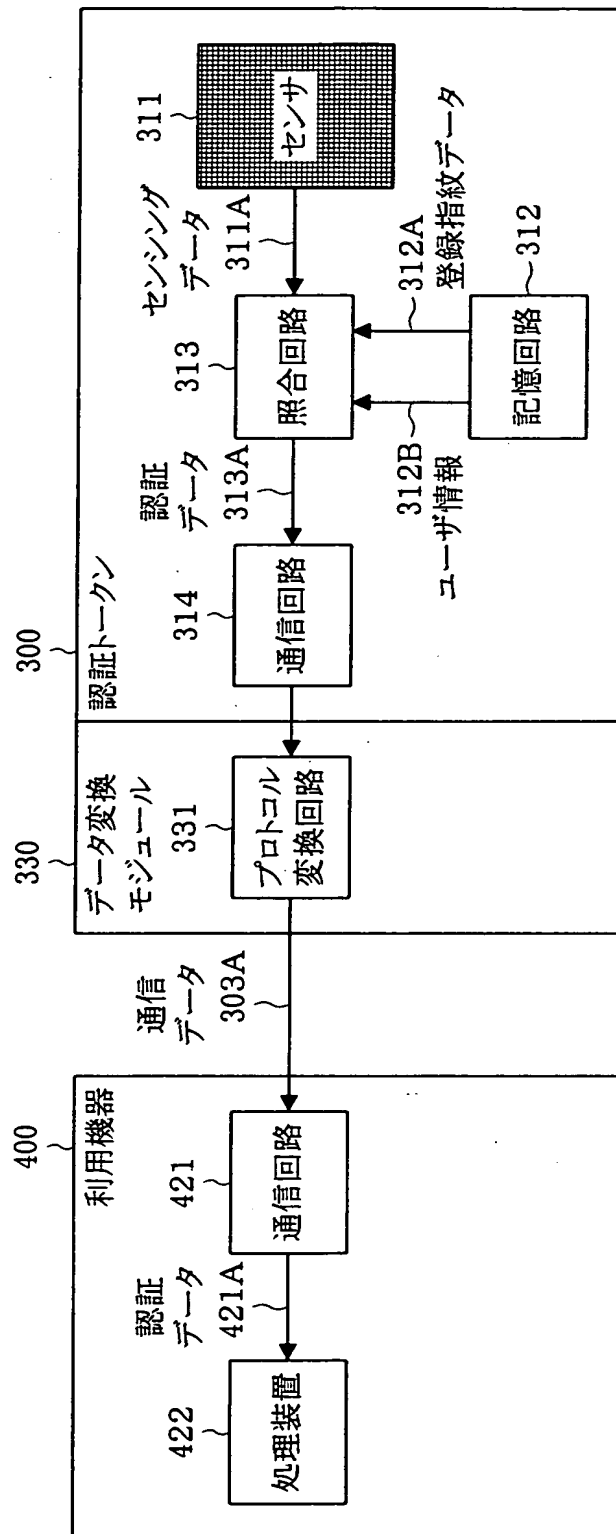
【図 7】



通信データ

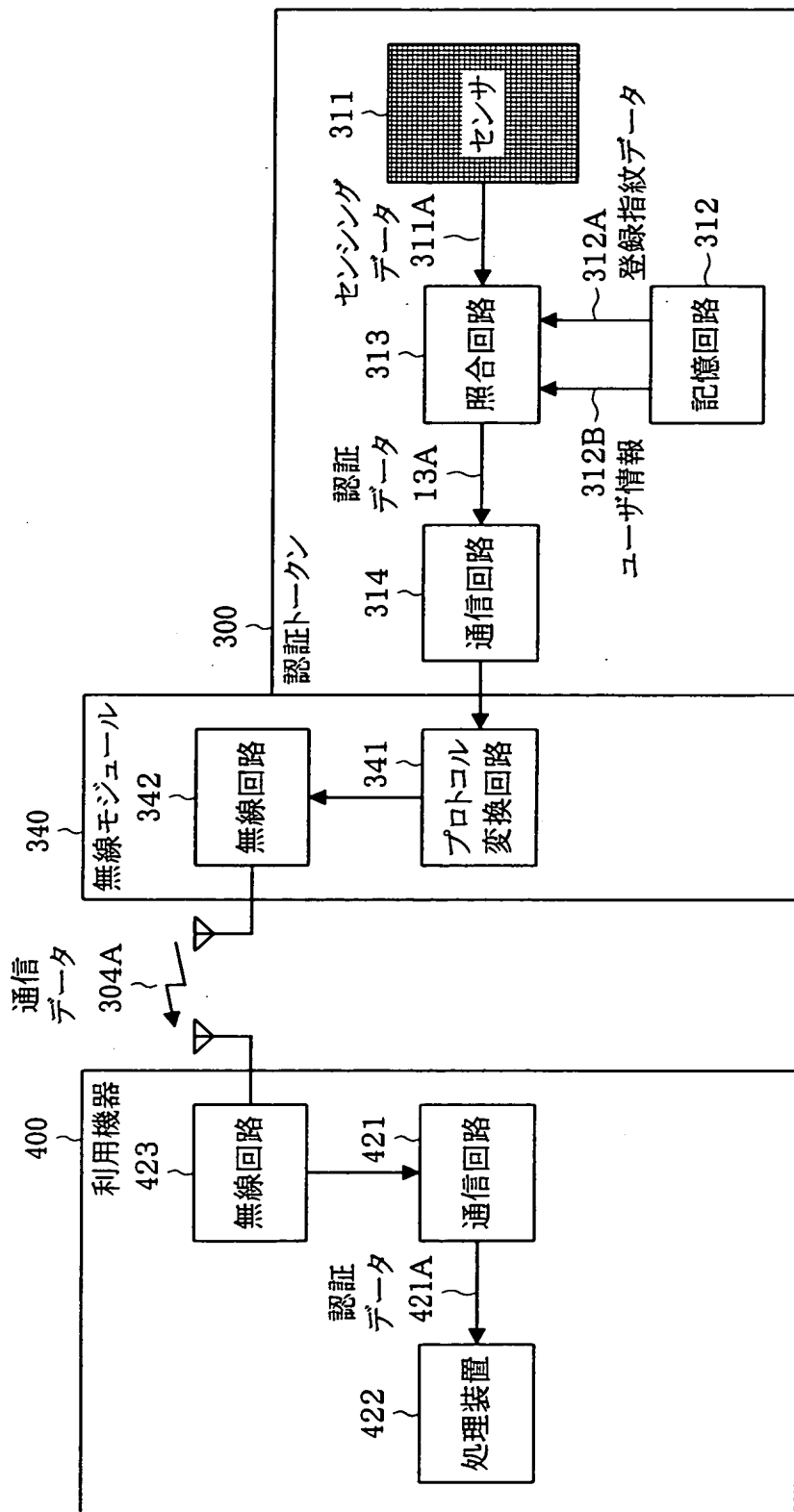
ユーザID
パスワード
照合結果
個人情報
⋮

【図 8】





【図 9】



【書類名】 要約書

【要約】

【課題】 利用者の指紋に基づき本人認証を行い利用者の現金の引き出しなど各種サービスを提供する場合、利用者の指紋データのセキュリティを向上させる。

【解決手段】 利用者が所有する指紋トークン200に利用者自身の指紋データを登録するとともに、利用者の口座番号を記憶し、指紋トークンの指紋センサ202が読み取った指紋データと登録データが一致すると、記憶している口座番号を自動現金受け払い機101へ送信し、自動現金受け払い機ではデータベース110からこの口座番号に対応する残高を取得しこの残高に応じた現金の払い出しを行う。

【選択図】 図3

出 願 人 履 歴 情 報

識別番号 [000004226]

1. 変更年月日	1999年 7月15日
[変更理由]	住所変更
住 所	東京都千代田区大手町二丁目3番1号
氏 名	日本電信電話株式会社